Abstract

This document describes a technique to generate valid DNSSEC answers on demand for non-existing names by claiming the name exists and returning a NSEC record for it. These answers require only one NSEC record and allow live-signing servers to minimize signing operations, packet size, disclosure of zone contents and required knowledge of the zone layout.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on September 22, 2016.

Copyright Notice

Copyright (c) 2016 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of

Section
Authenticated denial of existence went through several revisions
[RFC4034] [RFC5155] [RFC7129] with NSEC and NSEC3 currently deployed
in the wild. Both are designed to make offline signing possible, at
a time at which there is no knowledge of what names will be queried.
This leads to potentially unwanted disclosure of the zone contents.
NSEC3 tries to mitigate the disclosure by hashing the names, but zone
contents can still be recovered by a determined attacker.

Servers capable of generating signatures on demand (online signing)
instead have access to the name being queried when crafting the
denial of existence and can therefore produce answers that leak zero
information about the rest of the zone. Such a technique to be used
with NSEC records is presented in [RFC4470] ("Minimally Covering NSEC
Records") and one to be used with NSEC3 is documented in [RFC7129],
Appendix B ("NSEC3 White Lies").

The "Minimally Covering NSEC Records" technique involves dynamically
generating a NSEC record on a close predecessor and specifying a
close successor as the next name. A NSEC covering the wildcard name
must also be included, leading to two signed NSEC records (of which
one might be cached).

The "NSEC3 White Lies" technique involves dynamically generating a
NSEC3 record on the hash of the QNAME minus one and specifying the
hash of the QNAME plus one as the next name. NSEC3 matching the
closest encloser and covering the wildcard must also be included,
leading to three signed NSEC3 records (of which two might be cached).

There is a second type of secure negative answer, as opposed to a
NXDOMAIN: a NODATA, where the name queried for exists, but the type
does not. Common clients exhibit similar behaviors. Such an answer requires only one NSEC(3): the one with owner matching the QNAME, and no QTYPE in the bitmap.

The technique in this document exploits this observation and improves on the efficiency of existing live-signing schemes, by answering NODATA in place of NXDOMAIN, saving 1 or 2 NSEC(3) and their signatures.

1.1. Requirements

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2. Black Lies

Whenever a request for a non-existing name in a signed zone the server would be authoritative for is received, a NSEC record is generated with owner name matching the QNAME.

The next name SHOULD be set to the immediate lexicographic successor of the QNAME. Using a perfect epsilon function, such as the one in Section 3.1.2. of [RFC4471], allows the server not to require knowledge of any other names in the zone, as no other names are covered by the proof. This is particularly useful for servers that don’t have or want a complete view of the zone, like signing middlemen or key-value database backed servers.

The generated NSEC record’s type bitmap MUST have the RRSIG and NSEC bits set and SHOULD NOT have any other bits set. This mirrors [RFC4470] style ephemeral NSEC records.

For example, a request for the non-existing name a.example.com would cause the following NSEC record to be generated:

a.example.com. 3600 IN NSEC \000.a.example.com. ( RRSIG NSEC )

The answer MUST have RCODE NOERROR, as opposed to NXDOMAIN, since a record matching the QNAME is being returned.

Naturally, generated NSEC record MUST have corresponding RRSIGs generated.

A black lie requires only one signing operation, generates a single NSEC+RRSIG pair (which can commonly fit with a SOA+RRSIG in < 512 bytes), leaks no information on the rest of the zone and can be
generated knowing nothing else than the fact that the QNAME does not exist.

3. Side Effects of Sacrificing the NXDOMAIN RCODE

The main tradeoff of this technique is that NXDOMAIN answers are turned into NODATA, hiding the fact that the name does not exist. An intelligent client can recover part of this information by noticing the bitmap only carries (RRSIG NSEC), which indicates either a black lie or an empty non-terminal.

Large scale empirical observations suggest that clients behave in the same way faced with NXDOMAIN or NODATA, as they are usually uninterested in the DNS topology of the zone, but are only after a specific QNAME+QTYPE pair.

A server CAN decide to only turn NXDOMAIN into NODATA when the DO bit is set, so that older clients and clients interested in the topology of the zone for debugging purposes would still receive NXDOMAIN answers. This technique has been found not to cause any major issues in a large scale deployment. Otherwise, the server CAN decide to also turn NXDOMAIN into NODATA with DO=0 for consistency.

Never answering NXDOMAIN has the advantage that the server can drop empty non-terminal logic, as empty non-terminals would look the same as missing names. This again is useful for servers without a comprehensive view of the entire zone they are authoritative for.

Black lies effectively reverse the benefits of [I-D.ietf-dnsop-nxdomain-cut], unless a signaling system to distinguish black lies from empty non-terminals is agreed upon (TBD).

4. Security Considerations

The Security Considerations from [RFC4470] on online signing apply.

5. Acknowledgements

Dani Grant, Marek Majkowski, Vicky Shrestha, Nick Sullivan and Marek Vavrusa provided valuable comments.

6. References

6.1. Normative References
6.2. Informative References


Authors’ Addresses

Filippo Valsorda
CloudFlare Inc.
25 Lavington Street
London SE1 0NZ
UK

Email: filippo@cloudflare.com
Olafur Gudmundsson
CloudFlare Inc.
101 Townsend St.
San Francisco 94107
USA

Email: olafur@cloudflare.com